REMARKS

Reconsideration and allowance are respectfully requested in light of the above amendments and the following remarks.

A new Abstract is submitted herewith as required by the Office Action.

Claims 1-15 and 17-31 have been amended for punctuation, clarity, and to place all elements in non-means-plus-function format. The amendments are non-narrowing; therefore, no estoppel should be deemed to attach thereto. The amendments are believed to overcome the objections and indefiniteness rejections applied to the original claims.

Claims 1, 2, 4, 8-16, 19, 20, 24-28, and 31 stand rejected, under 35 USC §102(b), as being anticipated by Davis et al. (US 6,105,008). Claims 5-7, 17, 18, 21-23, 29, and 30 stand rejected, under 35 USC §103(a), as being unpatentable over Davis. Claim 3 stands rejected, under 35 USC §103(a), as being unpatentable over Davis in view of DiGiorgio et al. (US 6,385,729). The Applicants respectfully traverse these rejections.

The Applicants respectfully submit that Davis fails to anticipate the feature recited in claim 1 of a local client and a first server that have a first component for mutual authentication.

The Office Action proposes that Davis' client terminal 204 of Fig. 4 corresponds to the claimed local client and that Davis' payment server 206 corresponds to the claimed first server (see Office Action page 4, lines 20-22). Continuing, the Office Action proposes that Davis discloses (in column 13, line 47, through column 14, line 13) that client terminal 204 and payment server 206 have a first component for mutual authentication (page 4, lines 22-23).

However, Davis discloses the following with respect to client terminal 204 and payment server 206 in the cited portion of the specification and Fig. 11B. In step 620, a card 5 sends a success message 320 along with a card signature (which may be encrypted) back to a client module 224 in client terminal 204 (Davis col. 13, lines 64-66). This success message may also be termed a "debit response" message (col. 13, lines 66-67). At this point, the purchase amount has been deducted from the balance on stored-value card 5 (col. 13, line 67, through col. 14, line 2). Next, in step 622, client module 224 packages the success message along with the card signature and sends them back to payment server 206, as indicated at 322 (col. 14, lines 2-4). Client module 224 also logs the result of this stored-value card debit (col. 14, lines 4-6). In step 624, payment server 206 receives incoming message 322 and creates a log and updates the

transaction status in its database for future error recovery (col. 14, lines 7-9). Payment server 206 then directs this received message to a security card 218 in a terminal 214 as indicated at 324 (col. 14, lines 9-11). Next, in step 626, security card 218 processes this response from the client's terminal and verifies the received stored-value card signature (col. 14, lines 11-13). As the security card contains the keys and algorithms necessary to compute stored-value card signatures, the security card is able to validate that a received stored-value card signature is in fact a valid one by comparing this stored-value card signature with a generated expected value (col. 14, lines 14-18).

As may be determined from Davis' discussion above, Davis does not disclose that client terminal 204 and payment server 206 have a first component for mutual authentication. Although Davis may disclose in the cited portion of the specification that card 5 and security card 218 of terminal 214 may have matching cryptographic capabilities for encrypting/decrypting a communicated card signature, the Office Action proposes that Davis' security card 218 corresponds to the claimed HSM (see Office Action page 4, line 24, through page 5, line 2). Thus, Davis does not disclose the feature recited in claim 1 of a local

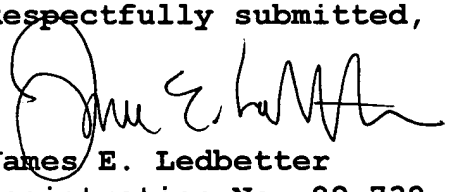
client and a first server that have a first component for mutual authentication.

Accordingly, the Applicants respectfully submit that Davis does not anticipate the subject matter defined by claim 1. Independent claim 19 similarly recites the above-mentioned feature distinguishing apparatus claim 1 from Davis, but with respect to a method. Therefore, allowance of claims 1 and 19 and all claims dependent therefrom is warranted.

In view of the above, it is submitted that this application is in condition for allowance and a notice to that effect is respectfully solicited.

If any issues remain which may best be resolved through a telephone communication, the Examiner is requested to telephone the undersigned at the local Washington, D.C. telephone number listed below.

Respectfully submitted,



Date: May 15, 2006
JEL/DWW/att

James E. Ledbetter
Registration No. 28,732

Attorney Docket No. L741.02102
STEVENS DAVIS, MILLER & MOSHER, L.L.P.
1615 L Street, N.W., Suite 850
P.O. Box 34387
Washington, D.C. 20043-4387
Telephone: (202) 785-0100
Facsimile: (202) 408-5200

--ABSTRACT OF THE DISCLOSURE

A system and method may provide a mechanism for performing secure configuration and data changes between a personal security device (PSD) and a hardware security module (HSM) using a communications pipe established between the PSD and the HSM. The data changes and configuration changes may include installing, updating, replacing, and deleting digital certificates, cryptographic keys, applets, digital credentials, attributes of installed objects, or stored proprietary information.--